AF/3621 #
IFW

P/1318-119

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS AND INTERFERENCES

In re Patent Application of:

	Robert BARRITZ et al.	Date	:	July 12, 2004
Serial No.	: 09/726,166	Group Art Unit	:	3621
Filed	: November 29, 2000	Examiner	:	David Q. Le
For	: LICENSE COMPLIANCE VERIFICATION SYSTEM			

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. §1.192

Sir:

This appeal is taken from the Examiner's final rejection dated January 9, 2004, in connection with the above-identified application. The Notice of Appeal was filed in the United States Patent and Trademark Office on May 10, 2004.

I. REAL PARTY IN INTEREST

The real party in interest in the above-identified application is:

ISOGON CORPORATION
330 7th Avenue
New York, New York 10001

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences of which Applicants are aware regarding the above-identified application.

07/15/2004 EAREGAY1 00000087 09726166
01 FC:2402 165.00 OP

III. STATUS OF CLAIMS

Claims 1-40 are pending the application and are on appeal herein.

Claims 1-40 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the patent to Bains et al. (U.S. Patent No. 5,579,222) in view of Ginter et al. (U.S. Patent No. 5,892,900).

IV. STATUS OF AMENDMENTS AFTER FINAL REJECTION

No Amendment After Final Rejection was filed.

V. SUMMARY OF THE INVENTION

As is widely known, the functionality and character of computers is substantially determined by the software products loaded into the computer to run at users' requests. Computers are typically loaded with hundreds if not thousands of different computer software products, provided by a large diversity of software vendors.

In large computer installations, the software products are subject to stringent license terms, e.g., the number of simultaneous users, the specific hardware on which the software may be run, the time usage that a licensee may make of the various software products, etc. In many instances, the users of the software products pay ongoing license fees that are determined on various usage criteria.

Computer installations, particularly at commercial business establishments, are controlled by one or more so-called "license managers" that exerts overall control over the requests to use licensed software products. The license manager determines whether the right-to-use is to be granted to specified users, whether the use being requested is within specified parameters and whether other criteria has been complied with. For example, a license manager might deny access to a particular user, or to particular software products, or to particular software products whose license has lapsed due to the limited time period for which a license has been granted.

The present invention is concerned with and addresses the situation that sometimes arises when users attempt to either tamper with license managers or attempt to utilize it in ways that are not contemplated by the various software licensors (vendors). Some license managers are designed to outrightly deny access whenever any irregularities is noted or on any attempt to

utilize a product outside of its precise licensing laws is encountered. But this has the potential of alienating customers or potential customers.

The present invention is not directed to a license manager *per se.* Rather, it provides a license compliance verification system that interfaces with a conventional license manager. That is, the claimed verification system includes the _____ license manager that internally monitors licensed software products and gathers data concerning usage of the licensed property including by reference to the various vendors of the licensed software. In other words, the license manager administers the licensed rights on a product by product basis so as to be able to provide reports that pertain to the different vendors of the different software products.

The novelty resides in that the claimed license compliance verification system also includes a monitoring software that interfaces with the license manager and extract from the license manager licensor-specific compliance data and authenticates that retrieved data against internal data so as to assure (based on the set of license-specific rules) that gathered software usage data by the (conventional) license manager has not been altered or improperly deleted and is being correctly reported to the software vendors.

By means of the present invention, the various computer software vendors are able to receive reports on the manner in which the local license manager administers their software products. They do not need to deny access to software and are able to make decisions regarding license rights at individual computer sites without being unduly intrusive on the day to day workings of computers, in a manner that is essentially hidden from the users.

VI. ISSUES TO BE DECIDED IN THIS APPEAL

The following issues is presented for review:

Whether claims 1-40 are unpatentable under 35 U.S.C. §103(a) over Bains et al. (U.S. Patent No. 5,579,222) in view of Ginter et al. (U.S. Patent No. 5,892,900).

VII. GROUPING OF CLAIMS

Claims 1-40 stand or fall together.

VIII. ARGUMENT

The Rejection of Claims 1- 40 Under 35 U.S.C. §103(a):

The license compliance verification system of claim 1 (and at the corresponding method of independent claim 17), is unique in the software licensing field in the following main respect. It is intended to allow each licensor, i.e. software vendor, among many different licensors, whose product is incorporated in a large computer data center to be individually provided with feedback or the assurance that the integrity of the local license manager has not been tampered with.

Many license managers are known that can handle the software applications of a large variety of licensors, i.e., of different software vendors. As is reflected by the prior art cited by the Examiner, it is known to have license managers that prevent tampering or defeating the license restrictions.

But no license manager is known or described in any of the two references of record which "gathers data and the usage of the licensed property... by reference to a plurality of licensors of the licensed property" (emphasis added).

Neither of the two references cited by the Examiner provides a special "monitoring software" that interfaces with the license manager and extracts from it "licensor-specific data" and/or which then authenticates the retrieved data "based on a set of licensor-specific rules".

As elsewhere provided in the claims, that specific information is then routed to the various licensors, whereby they obtain a feedback, which confirms the integrity and reliability of the local license manager.

The primary Bains reference describes an active "license manager" which dynamically (and online) manages the retrieving of application software through the logging, controlling and supervising the usage of licensed software. As described in the abstract of the Bains reference, the licensor identifies the current set of nodes that are using the software product and handles license data concerning conditions under which usage of the software product is permitted at any given node. Thereby, "the software product may thus include instructions to interface with the license server to cause enforcement of the licensed terms."

Ginter et al. is concerned with a license manager that is capable of administrating licenses "distributed over a virtual distribution environment (VDE)". It provides an "electronic highway" for administering licenses.

Neither of these references is designed for, nor discloses any mechanism or procedure for providing assurances to licensors that the operations of the local license manager have not been tampered with to defeat its functionality. It is at least possible that a sophisticated software operator might defeat the safeguards of the license manager of the Bains reference or of the VDE system of Ginter et al. and the licensors would never know this, because the licensors never get any feedback and information from the license manager which the present invention provides via an added layer of checks that produces results that are communicated to the licensors based on the specific rules of different licensors for the purpose of verification. With the invention, defeating the license manager is closer to being impossible.

Accordingly, it is submitted that claims 1 and 17 are clearly directed to patentable subject matter and so are all the remaining claims in the application, since each depends from one or the other of the independent claims and imposes further limitations thereon.

Contrary to the Examiner, Claim 1 is not about a "plurality of licensors". It is directed to a "license compliance verification system". It is not a license manager *per se*. Its function is not to grant rights to requesters to use a particular product based on any specific criteria. Resident license managers do that.

The Examiner directs the applicant to Bains Figure 1 and to the associated text at column 5, lines 28-35. Several important observations must be made. The cited text, including as quoted in the Office Action: "...running a variety of software products, such as PDS (item 12a), EMS (item 12b), and so forth (shown through item 12j)." does not at all teach (one way or another) a reference to a "plurality of licensors". IBM sells hundreds of different software products and a system can have 100 IBM software products all dealing with a single, rather than a plurality of, licensors.

Part and parcel of claim 1 is a license compliance verification system that comprises a license manager that internally monitors use of license property and, most significantly, "gathers data on the usage of the licensed property, including by reference to a plurality of licensors of the licensed property."

Bains does not disclose gathering data on the usage of licensed property. It is the license manager itself that monitors requests for usage of licensed property and grants the right to use the licensed property based on certain criteria.

The system of Bains further does not have the claimed "monitoring software" which, among other things, "interfaces with the license manager and extracts from it license or specific data and authenticates the retrieved data, such that licensors are assured, based on a set of license-specific rules that data gathered by the license manager has not been altered or improperly deleted prior to its being provided to licensors."

Bains does not communicate with licensors. Bains does not provide data to licensors. Bains does not carry out any step and contains no disclosure of the utility or reason for gathering data and most significantly, "authenticating" the retrieved data such that licensors are assured that the data provided by the license manager *per se*, has not been altered or improperly deleted prior to its being provided to licensors. None of the foregoing steps and features are disclosed in Bains. Bains and the present invention verily relate to the proverbial apples and oranges, respectively.

In the typical license manager, if a user's request for a license does not fall within a specific criteria, the right to use the software will be denied. As pointed out at pages 3-7 of the instant specification, many license systems simply deny or take specific measures against improper use of software. The present invention specifically does not want to tamper or interfere with the user's rights or pleasure of using the software. They simply want to report to the licensor on the usage of the software, but include the step that will report out of conformance usages of their software to the licensor. Bains does not do that, nor does it have any disclosure of the desirability of doing so, nor of how it may be implemented. All of the foregoing features and elements are, in contrast, provided for in claim 1 and in the many remaining claims of the instant application. For example, claim 5 specifically states that the gathered data is out of compliance data. What the Office Action has done with respect to that limitation, is simply reason its way to the conclusion that using Ginter would "inherently save all instances of out of compliance license requests as well." Claim 1 calls for authentication of information based on specific rules. Respectfully, nowhere in the rules can one find any disclosure of testing the granting of license on the basis of specific rules in the manner set forth in the main independent claim of the present

application. Therefore, the main independent claims 1 and 17 are patentable over the prior art and all the remaining claims which include its limitation are patentable as well.

IX. CONCLUSION

Accordingly, in view of the above considerations, it is Applicants' position that the Examiner's rejection of claims 1-40 under 35 U.S.C. §103(a) over Bains et al. (U.S. Patent No. 5,579,222) in view of Ginter et al. (U.S. Patent No. 5,892,900), is in error and should be reversed.

Our check No. 17447, which includes the amount of $165.00, for a small entity, to cover the appeal brief is attached hereto. This brief is being submitted in triplicate in accordance with 37 C.F.R. 1.192 and applicant reserves the right to request an oral hearing upon receipt of the Examiner's Answer.

If this communication is being filed after a shortened statutory time period has elapsed and no separate Petition is enclosed, the Commissioner of Patents and Trademarks is petitioned, under 37 C.F.R. §1.136(a), to extend the time for filing the required papers by the number of months which will avoid abandonment under 37 C.F.R §1.135. The fee under 37 C.F.R. §1.17 should be charged to our Deposit Account No. 15-0700.

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Mail Stop Appeal Brief, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on July 12, 2004

Max Moskowitz
Name of applicant, assignee or Registered Representative

Signature

July 12, 2004
Date of Signature

MM:msd

Respectfully submitted,

Max Moskowitz
Registration No.: 30,576
OSTROLENK, FABER, GERB & SOFFEN, LLP
1180 Avenue of the Americas
New York, New York 10036-8403
Telephone: (212) 382-0700

APPENDIX A

CLAIMS ON APPEAL

1. A license compliance verification system, comprising:

a license manager that internally monitors use of licensed property, intended to be used by licensed users, and gathers data on the usage of the licensed property including by reference to a plurality of licensors of the license property; and

monitoring software that interfaces with the license manager and extracts from it licensor-specific data and authenticates the retrieved data such that licensors are assured, based on a set of license-specific rules, that data gathered by the license manager has not been altered or improperly deleted prior to its being provided to licensors.

2. The license compliance verification system of claim 1, in which the licensed property comprises computer software.

3. The license compliance verification system of claim 1, in which the monitoring software includes a facility that enables users to review data before it is sent to licensors and prevents users from modifying such data.

4. The license compliance verification system of claim 1, in which the license manager includes a facility that accepts passwords and license certificates for authorizing usage of respective ones of the licensed property.

5. The license compliance verification system of claim 1, in which the gathered data comprises out-of- compliance data.

6. The license compliance verification system of claim 1, in which the gathered data comprises license certificate modification data.

7. The license compliance verification system of claim 1, in which the monitoring software includes a facility that enables licensors to directly and remotely provide instructions to the monitoring software.

8. The license compliance verification system of claim 1, in which direct access to the monitoring software is granted to an agent operating on behalf of a licensor but which is active on a user's computer.

9. The license compliance verification system of claim 1, further including an operator control facility that enables controlling the monitoring software to carry out a data gathering task based on selection criteria and the selection criteria includes at least identification of products or licensors.

10. The license compliance verification system of claim 1, in which the monitoring software is operable on a time scheduling basis.

11. The license compliance verification system of claim 1, further including a facility for creating a new symmetric encryption key for encrypting the data to be transferred to licensors.

12. The license compliance verification system of claim 11, including a facility that encrypts the symmetric encryption key using a public key of a licensor.

13. The license compliance verification system of claim 11, including a facility that encrypts the symmetric encryption key using a public key of a user.

14. The license compliance verification system of claim 1, further including an authenticating facility which is operable as a part of the monitoring software and which authenticates data that is gathered for a licensor, to prevent tampering with such data.

15. The license compliance verification system of claim 14, in which the authentication comprises a message digest and the message digest is a data digest selected from the group consisting of

a hash value or an arithmetic total computed from encrypted data which is then encrypted using a private key specific to the monitoring software.

16. The license compliance verification system of claim 1, in which the licensed property is selected from a property group consisting of: licensed software, trade secrets, copyrighted music, copyrighted books, copyrighted photos, copyrighted movies, and copyrighted videos.

17. A method for verifying compliance with license conditions, the method comprising the steps of:

operating a license manager so as to internally monitor use of licensed property, intended to be used by licensed users, and gathering data on the usage of the licensed property including by reference to respective licensors of the licensed property; and

extracting, from data logged by the license manager, licensor-specific data; and authenticating at least portions of the retrieved data based on licensor-specific rules in preparation for forwarding the retrieved data to one or more licensors, so as to assure that data gathered by the license manager has not been altered or improperly deleted prior to its being provided to licensors.

18. The method of claim 17, in which licensed property comprises computer software.

19. The method of claim 17, further including enabling users to review data before it is sent to licensors and preventing users from improperly modifying such data.

20. The method of claim 17, including operating the license manager to accept passwords and license certificates for authorizing usage of respective ones of the licensed property.

21. The method of claim 17, including retrieving from the license manager out-of-compliance data.

22. The method of claim 17, in which the gathered data comprises license certificate modification data.

23. The method of claim 17, including enabling licensors to directly and remotely provide instructions which affect the retrieving of data from the license manager.

24. The method of claim 23, further including operating an agent on behalf of the licensor which is active on a user's computer.

25. The method of claim 17, further including controlling the retrieving of data from the license manager based on selection criteria that select information at least on a basis of identifying licensors or licensed products.

26. The method of claim 17, further including retrieving data from the license manager by reference to time periods over which such data has been initially collected.

27. The method of claim 17, further including creating a new symmetric encryption key for encrypting the data to be transferred to licensors.

28. The method of claim 27, including encrypting the symmetric encryption key using the public key of the licensor.

29. The method of claim 27, including encrypting the symmetric encryption key using the public key of a user.

30. The method of claim 17, further including authenticating retrieved data.

31. The method of claim 30, including employing an authentication process which comprises including a message digest, said message digest being a data digest selected from a group consisting of a hash value or an arithmetic total computed from the encrypted data which is encrypted using a private key.

32. The method of claim 17, in which the licensed property is selected from a property group consisting of: licensed software, trade secrets, copyrighted music, copyrighted books, copyrighted photos, copyrighted movies and copyrighted videos.

33. The method of claim 28, further including encrypting the symmetric encryption key which has been encrypted using the public key of the licensor, with a user's public key and subsequently providing such twice encrypted information to a respective user.

34. The license compliance verification system of claim 12, including a facility that encrypts the symmetric encryption key, which has been encrypted using the public key of the licensor, with a user's public key and subsequently providing such twice encrypted information to a respective user.

35. The license compliance verification system of claim 1, further including a central clearinghouse facility, the monitoring software accumulating licensor-specific data pertaining to a plurality of licensors and transmitting the same to the central clearinghouse facility, the clearinghouse facility consolidating, sorting and providing the licensor-specific data according to licensors.

36. The license compliance verification system of claim 35, in which the monitoring software and the central clearinghouse facility interact with each other automatically.

37. The license compliance verification system of claim 35, in which the monitoring software and the central clearinghouse facility interact with each other in response to prompting by specific licensors.

38. The method of claim 17, further including accumulating the licensor-specific data relative to a plurality of licensors and transmitting the same to a central clearinghouse facility, the central clearinghouse facility consolidating, sorting and providing the licensor-specific data according to licensors.

39. The method of claim 38, including transmitting the licensor-specific data to the central clearinghouse facility automatically.

40. The method of claim 38, including transmitting the licensor-specific data to the central clearinghouse facility in response to prompting by specific licensors.